Modular Arithmetic.

Divisibility:-

The set of integers consists of all positive integers, all negative integers and zero. It is denoted by I or Z.

I or Z = $\{ \dots -3, -2, -1, 0, 1, 2, 3 \dots \}$

$= \{0, \pm1, \pm2, \pm3, \pm4, \pm5, \dots\}$

Consider 2 integers a and b where $a \neq 0$, a divides b if there exists an integer k such that $b = k.a$.

Eg:- 9 divides 54 ; there is the integer 6 such that

$54 = 6 \times 9$.

'a divides b' is written as $a|b$ (the symbol '|' stands for divides).

Eg:- i) $13|-52$ $\because$ $-52 = -4 \times 13$

ii) $9 \nmid 78$ (9 does not divide 78)

$78 \neq$ (an integer) 9

Division Algorithm :-

Given two integers a and b where $a > 0$, two unique integers q and r can always be found such that $b = qa + r$, where $0 \leq r < a$. This is known as division algorithm. q is called the quotient and r is called the remainder.

The process of division is as follows:

$$a)\, b\,(\,q$$
$$\frac{qa}{b - qa = r}, \quad \text{Where } 0 \leq r < a.$$

i.e $b = qa + r$, $0 \leq r < a$.

In case $r = 0$, $b = qa \Rightarrow a|b$.

Dr. Sreelakshmi
BMSIT&M

9:-

1) $a=25,\ b=18$

$$25\overline{)18}(0$$
$$\begin{array}{r} 18 \\ \underline{00} \\ 18 \end{array}$$

$\therefore q=0,\ r=18$ $\quad$ $\therefore \underline{18 = 0\times25+18.}$

2) $a=17,\ b=2589$

$$17\overline{)2589}(152$$
$$\begin{array}{r} 2589 \\ \underline{17} \\ 88 \\ \underline{85} \\ 39 \\ \underline{34} \\ 5 \end{array}$$

$\therefore q=152,\ r=5$ $\quad$ $\therefore \underline{2589 = 152\times17+5.}$

3) $a=17,\ b=-245$

$$17\overline{)-245}(-15$$
$$\begin{array}{r} -245 \\ \underline{-255} \\ 10 \end{array}$$

$\therefore q=-5,\ r=10$ $\quad$ $\therefore \underline{-245 = -15\times17+10.}$

*Note:-

In all divisions q may be positive or negative or zero; but r is always positive (or zero) and less than the divisors.

* Greatest Common Divisor (G.C.D) OR Highest Common Factor (H.C.F).

The G.C.D of two integers a and b (both of them are not zero) is a unique positive integer d such that

i) d is the common divisor of both a and b,
 i.e, $d|a$, $d|b$.

ii) every common divisor of a and b divides d
 i.e $x|a$ and $x|b \Rightarrow x|d$.

The G.C.D of 2 numbers a and b is written as (a,b) i.e, $d=(a,b)$.

Eg:- Consider the integers 12 and 18.
The positive divisors of 12 are 1, 2, 3, 4, 6, 12.
The positive divisors of 18 are 1, 2, 3, 6, 9, 18.
the common divisors of 12 and 18 are 1, 2, 3, 6
clearly 6 is the G.C.D of 12 and 18.
i) 6 is the common divisor of 12 and 18
 i.e., $6|12$, $6|18$.
ii) every common divisior of 12 and 18 divides 6.
 i.e $1|6$, $2|6$, $3|6$ and $6|6$.

---

* Euclid's Algorithm method to find the G.C.D of 2 given numbers a and b and to express the G.C.D as $ax+by$.

A method of finding the greatest common divisor of two numbers by dividing the larger by the smaller, the smaller, the smaller by the remainder, the first reminder by the second remainder, and so on until exact division is obtained hence the greatest common divisor is the exact divisor.

∴ Steps to find gcd using Euclidian Algorithm for any two integers a and b with $a > b$.

Step 1: Let a, b be the two numbers.
Step 2: $a \bmod b = R$.
Step 3: Let $a = b$ and $b = R$.
Step 4: Repeat steps 2 and 3 until $a \bmod b$ is greater than 0.

---

1) Find the G.C.D of 32 and 54 and express it in the form $32x + 54y$.

$$32\,)\,54\,(\,1 \qquad 54 - 32 = 22$$

$$22 = 54 - 1(32) \rightarrow (1)$$

$$22\,)\,32\,(\,1 \qquad 32 - 22 = 10$$

$$10 = 32 - 1(22) \rightarrow (2)$$

$$10\,)\,22\,(\,2 \qquad 22 - 20 = 2$$

$$2 = 22 - 2(10) \rightarrow (3)$$

$$2\,)\,10\,(\,5 \qquad 10 - 10 = 0$$

∴ The last non zero remainder is 2.

∴ G.C.D is 2.

From (3),

$$2 = 22 - 2(10)$$

$$2 = [54 - 1(32)] - 2[32 - 1(22)]$$

$$2 = 54 - 3(32) + 2(22)$$

$$= 54 - 3(32) + 2[54 - 1(32)]$$

$$= 3(54) - 5(32)$$

$$= 54(3) + 32(-5)$$

i.e $2 = 54x + 32y$ Where $x = 3, y = 5$.

Find the G.C.D of 25520 and 19314 and express it in the form $25520x + 19314y$.

$$\begin{array}{r} 19314\overline{)25520}(1 \\ 19314 \\ \hline 6206 \end{array}$$

$6206 = 25520 - 1(19314) \rightarrow (1)$

$$\begin{array}{r} 6206\overline{)19314}(3 \\ 18618 \\ \hline 696 \end{array}$$

$696 = 19314 - 3(6206) \rightarrow (2)$

$$\begin{array}{r} 696\overline{)6206}(8 \\ 5568 \\ \hline 638 \end{array}$$

$638 = 6206 - 8(696) \rightarrow (3)$

$$\begin{array}{r} 638\overline{)696}(1 \\ 638 \\ \hline 58 \end{array}$$

$58 = 696 - 1(638) \rightarrow (4)$

$$\begin{array}{r} 58\overline{)638}(11 \\ 638 \\ \hline 0 \end{array}$$

$\therefore$ The last non-zero remainder is 58.

$\therefore$ G.C.D is 58.

From (4),

$58 = 696 - 1(638)$.

$58 = 696 - 1[6206 - 8(696)]$

$58 = 9 \times 696 - 6206$.

$58 = 9[19314 - 3(6206)] - 6206$

$58 = 9 \times 19314 - 28 \times 6206$.

$58 = 9 \times 19314 - 28[25520 - 1(19314)]$

$58 = 37 \times 19314 - 28 \times 25520$.

$58 = (-28)25520 + (37)19314$.

i.e $58 = 25520x + 19314y$ where

$x = -28$, $y = 37$.

Relatively Prime numbers:

Two numbers a and b are said to be relatively prime or co-prime if and only if $(a,b)=1$, i.e the g.c.d of a and b is 1.

Eg: $(8,15)=1$ $\therefore$ 8 and 15 are relatively prime.

---

* Congruences:

Let m be a positive integer (>1). If a and b are any integers then a is said to be congruent to b modulo m if and only if $m \mid a-b$.

'a is congruent to b modulo m' is written as

$a \equiv b \pmod m$.

Thus if $a \equiv b \pmod m$ then $m \mid a-b$ and conversely if $m \mid a-b$ then $a \equiv b \pmod m$.

Eg: i) $25 \equiv 3 \pmod{11}$ $\quad 11 \mid 25-3$ ie, $11 \mid 22$.

ii) $-69 \equiv -5 \pmod{16}$ $\quad 16 \mid -69+5$ ie, $16 \mid 64$

iii) $79 \not\equiv 8 \pmod 9$ $\quad 9 \nmid 79-8$.

* Consider the congruence $134 \equiv 108 \pmod{13}$ which is true.

$$13)134(10 \qquad 13)108(8$$
$$\underline{130} \qquad \underline{104}$$
$$4 \qquad 4.$$

When 134 and 108 are divided by 13, the same remainder 4 is obtained. This gives the alternate definition of the congruence.

Defn:- If m is a positive integer (>1) and a and b are any integers then 'a' is said to be congruent to b modulo m if and only if a and b leave the same remainder when divided by m.

Eg:- i) $45 \equiv 3 \pmod 4$

$45 - 3 = 42$, $4 \nmid 42$ $\therefore$ It is false.

ii) $-124 \equiv -172 \pmod{12}$

$-124 + 172 = 48$, $12 \mid 48$ $\therefore$ It is true.

iii) $2^8 \equiv 1 \pmod{17}$

$2^8 - 1 = (2^4)^2 - 1 = 256 - 1 = 255$, $17 \mid 255$ $\therefore$ It is true.

Problems:

1) Solve $5x \equiv 4 \pmod{13}$

$\Rightarrow 13 \mid 5x - 4$

$\Rightarrow 5x - 4 = 13K$ where $K \in \mathbb{Z}$

$\Rightarrow 5x = 13K + 4$

$\Rightarrow x = \frac{13K+4}{5}$

By inspection, $K=2$ gives the integral value of x.

i.e, $x = \frac{13(2)+4}{5} = 6$.

i.e $x \equiv 6 \pmod{13}$ $\therefore$ The general solution is $x = 6 + 13t$ where $t \in \mathbb{Z}$.

---

2).

If $2^8 \equiv a \pmod{13}$ find a.

$2^8 = (2^4)^2 = 256$

$\therefore$ $256 \equiv 9 \pmod{13}$

i.e, $2^8 \equiv 9 \pmod{13}$ $\therefore$ $a = 9$.

$$\begin{array}{r} 13\overline{)256}(19 \\ \underline{13} \\ 126 \\ \underline{117} \\ 9 \end{array}$$

---

3) Solve $7x \equiv 9 \pmod{15}$

$\Rightarrow 15 \mid 7x - 9$

$\Rightarrow 7x - 9 = 15K$

$\Rightarrow 7x = 15K + 9$ where $K \in \mathbb{Z}$

$\Rightarrow x = \frac{15K+9}{7}$

By inspection, $K=5$ gives the integral value of x.

i.e $x = \frac{15(5)+9}{7} = \frac{75+9}{7} = 12$.

$\therefore$ $x \equiv 12 \pmod{15}$

4) Find the least positive values of x such that

i) $71 \equiv x \pmod 8$

$$8\overline{)71}(8$$
$$\frac{64}{7}$$

The value of $\underline{\underline{x = 7}}$.

ii) $78 + x \equiv 3 \pmod 5$

$78 + x - 3 = 5n$ (n is any integer)

$75 + x = 5n$

Let $x = 5$

$75 + 5 = 80$ (80 is multiple of 5)

$\therefore$ The least value of x is 5

iii) $89 \equiv (x+3) \pmod 4$

$89 - x - 3 \equiv 4n$

$86 - x = 4n$

Let $x = 2$.

$86 - 2 = 84$ (84 is multiple of 4)

$\therefore$ The least value of x is 2.

iv) $96 \equiv \left(\frac{x}{7}\right) \bmod 5$.

$96 - \frac{x}{7} = 5n$

$672 - x = 35n$

$672 - 7 = 665$ (multiple of 35 is 665)

$\therefore$ The value of $x = 7$

v) $5x \equiv 4 \pmod 6$

$5x - 4 = 6n$

$5x = 6n + 4$

$x = \frac{6n+4}{5}$

Substitute the value of n as $1, 6, 11, 16 \ldots$ as n values is $x = (6n+4)/5$ which is divisible by $2, 8, 14, 20 \ldots$

$\therefore$ The least positive value is 2.

---

5) If $2x \equiv 3 \pmod 7$ find x such that $9 \leq x \leq 30$.

$x = 5$ satisfies the congruence because $10 \equiv 3 \pmod 7$ is true.

$\therefore x \equiv 5 \pmod 7$ is the solution.

Solution set $= \{ \ldots -9, -2, 5, 12, 19, 26, 33, \ldots \}$

The required values of x are 12, 19, 26.

---

6) Find the least positive remainder when 2^{301} is divided by 5.

$2^4 = 16 \equiv 1 \pmod 5$

$(2^4)^{75} \equiv 1 \pmod 5$

$$\begin{array}{r|l} 4 & 301 \,(75 \\ & \underline{28} \\ & 21 \\ & \underline{20} \\ & 1 \end{array}$$

$2^{300} \equiv 1 \pmod 5 \rightarrow ①$

$2 \equiv 2 \pmod 5 \rightarrow ②$

① × ②

$2^{301} \equiv 2 \pmod 5$

$\therefore$ Remainder is 2

---

7) Find the unit digit in the number 7^{289}.

$7^2 \equiv 9 \pmod{10}$

$7^4 \equiv 81 \equiv 1 \pmod{10}$

$(7^4)^{72} \equiv 1 \pmod{10}$

$7^{288} \equiv 1 \pmod{10}$

$7 \equiv 7 \pmod{10}$

$7^{289} \equiv 7 \pmod{10}$

$$\begin{array}{r} 4\,)\,289\,(72 \\ \underline{28} \\ 9 \\ \underline{8} \\ 1 \end{array}$$

$\therefore$ unit digit in 7^{289} is 7.

---

8) Find the last digit of 7^{2013}.

$7^2 \equiv 9 \pmod{10}$

$7^4 \equiv 81 \equiv 1 \pmod{10}$

$(7^4)^{503} \equiv 1 \pmod{10}$

$7^{2012} \equiv 1 \pmod{10}$

$7 \equiv 7 \pmod{10}$

$\therefore 7^{2013} \equiv 7 \pmod{10}$

$$\begin{array}{r} 4\,)\,2013\,(503 \\ \underline{20} \\ 13 \\ \underline{12} \\ 1 \end{array}$$

$\therefore$ last digit is 7

---

1) Find the unit(last) digit in the number 7^{126}.

$7^2 \equiv 9 \pmod{10}$

$7^4 \equiv 81 \equiv 1 \pmod{10}$

$(7^4)^{31} \equiv 1 \pmod{10}$

$7^{124} \equiv 1 \pmod{10}$

$7^2 \equiv 9 \pmod{10}$

$7^{126} \equiv 9 \pmod{10}$.

$\therefore$ 9 is the unit digit in 7^{126}.

$$\begin{array}{r|l} 4 & 126 \,(31 \\ & \underline{12} \\ & \ \ 6 \\ & \ \ \underline{4} \\ & \ \ 2 \end{array}$$

---

10) Find the last digit of 13^{37}.

$13 \equiv 13 \pmod{10}$

$13 \equiv 3 \pmod{10}$

$13^2 \equiv 3^2 \pmod{10}$

$13^2 \equiv 9 \pmod{10}$

$\equiv -1 \pmod{10}$

$13^4 \equiv (-1)^2 \pmod{10}$

$13^4 \equiv 1 \pmod{10}$

$(13)^{37} \equiv 13^{4\times9+1} = 13^{4\times9} \cdot 13$

$= (13^4)^9 \cdot 13$

$= 1 \bmod 10 \times 13$

$= 13 \bmod 10$

$(13)^{27} = 3 \bmod 10$

$\therefore$ 3 is the last digit in 13^{37}.

11.) What is the remainder in the division of 2^{50} by 7?

$2^3 = 8 \equiv 1 \pmod 7$

$(2^3)^{16} \equiv 1^{16} \pmod 7 \rightarrow (1)$

$2^2 \equiv 4 \pmod 7 \rightarrow (2)$

$2^{48} \cdot 2^2 \equiv 1 \cdot 4 \pmod 7$

$\therefore 2^{50} \equiv 4 \pmod 7$

$\therefore$ the remainder is 4.

---

*12) Find the remainder when 2^{23} is divided by 47.

$2^8 \equiv 256 \equiv 21 \pmod{47}$

47)256(5
235
21

$(2^8)^2 \equiv (21)^2 \pmod{47}$

$2^{16} \equiv 441 \pmod{47}$

47)441(9
423
18

$2^{16} \equiv 18 \pmod{47} \rightarrow (1)$

$2^7 \equiv 128 \equiv 34 \pmod{47} \rightarrow (2)$

47)128(2
94
34

(1) $\times$ (2)

$2^{16} \times 2^7 = 18 \times 34 \pmod{47}$

$2^{23} \equiv 612 \pmod{47}$

47)612(13
47
142
141
1

$2^{23} \equiv 1 \pmod{47}$

$\therefore$ the remainder is 1.

Find the remainder when $135 \times 74 \times 48$ is divided by 7.

$$7)\,135\,(19$$
$$\begin{array}{r} 7 \\ \hline 65 \\ 63 \\ \hline 2 \end{array}$$

$135 \equiv 2 \pmod 7 \rightarrow (1)$

$$7)\,74\,(10$$
$$\begin{array}{r} 70 \\ \hline 4 \end{array}$$

$74 \equiv 4 \pmod 7 \rightarrow (2)$

$$7)\,48\,(6$$
$$\begin{array}{r} 42 \\ \hline 6 \end{array}$$

$48 \equiv 6 \pmod 7 \rightarrow (3)$

1 × 2 × 3

$135 \times 74 \times 48 \equiv 48 \pmod 7 \equiv 6 \pmod 7$

$\therefore$ the remainder is 6

---

14) Find the remainder obtained when $64 \times 65 \times 66$ is divided by 67.

$64 \equiv -3 \pmod{67} \rightarrow (1)$
$65 \equiv -2 \pmod{67} \rightarrow (2)$
$66 \equiv -1 \pmod{67} \rightarrow (3)$

1 × 2 × 3

$64 \times 65 \times 66 \equiv -6 \pmod{67}$
$\equiv 61 \pmod{67}$

$\therefore$ the remainder is 61

---

15) Find the remainder when $349 \times 74 \times 36$ is divided by 3.

$$3)\,349\,(116$$
$$\begin{array}{r} 3 \\ \hline 49 \\ 3 \\ \hline 19 \\ 18 \\ \hline 1 \end{array}$$

$349 \equiv 1 \pmod 3 \rightarrow (1)$

$$3\overline{)74}(24$$
$$\frac{6}{14}, \quad \frac{12}{2}$$

$74 \equiv 2 \pmod 3 \rightarrow (2)$

$$3\overline{)36}(12$$
$$\frac{36}{0}$$

$36 \equiv 0 \pmod 3 \rightarrow (3)$

① × ② × ③

$349 \times 74 \times 36 \equiv 0 \pmod 3$

$\therefore$ the remainder is 0.

---

16) Find the reminder when $175 \times 113 \times 53$ is divided by 11.

$$11\overline{)175}(15$$
$$\frac{11}{65}, \quad \frac{55}{10}$$

$175 \equiv 10 \pmod{11} \rightarrow (1)$.

$$11\overline{)113}(10$$
$$\frac{110}{3}$$

$113 \equiv 3 \pmod{11} \rightarrow (2)$

$$11\overline{)53}(4$$
$$\frac{44}{9}$$

$53 \equiv 9 \pmod{11} \rightarrow (3)$

① × ② × ③

$175 \times 113 \times 53 = 10 \times 3 \times 9 \equiv 270 \pmod{11}$

$\equiv 6 \pmod{11}$

$\therefore$ the remainder is 6

**17) Find the remainder when the number 2^{1000} is divided by 13.

$2 = 2$; $2^2 = 4$; $2^3 = 8$, $2^4 = 16 \equiv 3 \pmod{13}$

$2^5 = 32$, $2^6 \equiv 64 \equiv -1 \pmod{13}$

$2^{1000} = 2^{6 \times 166 + 4}$.

$= (2^6)^{166} \cdot 2^4$.

$\equiv (-1)^{166} \bmod 13 \cdot 3 \bmod 13$

$= 1 \bmod 13 \cdot 3 \bmod 13$

$2^{1000} \equiv 3 \bmod 13$

$$\begin{array}{r} 6\overline{)1000}(166 \\ \underline{6} \\ 40 \\ \underline{36} \\ 40 \\ \underline{36} \\ 4 \end{array}$$

$\therefore$ The remainder is 3.

* Rules for finding x in linear congruence:

General format : $ax \equiv b \pmod{n}$.

1) Find $gcd(a, n) = d$ (let)
2) b/d → if possible → Solution exist.
3) Find $d \bmod n$ → There no. of sol^n are possible.
4) Divide both sides by d.
5) Multiply both sides by 'Mul. inverse of a'.
   ie $(a a^{-1})x = b.a^{-1} \pmod{n}$
6) General sol^n eq^n is
   $$x_k = x_0 + k\left(\frac{n}{d}\right),$$
   Where $k = \{0, 1, 2 \ldots (d-1)\}$.

---

1) $14x \equiv 12 \pmod{18}$

   $ax \equiv b \pmod{n}$

   $a = 14,\ b = 12,\ n = 18$.

1) $gcd(a, n) \rightarrow d$
   $gcd(14, 18) = 2$ (d)
2) $b/d = 12/2 = 6$ → Sol^n exist.
3) $d \bmod n = 2 \bmod 18 = 2$ → 2 sol^n exist.
4) Divide both the sides by d.
   $$\frac{14}{2}x \equiv \frac{12}{2} \left(\bmod \frac{18}{2}\right)$$
   $$7x \equiv 6 \pmod{9}$$
5) Multiply both sides by mul. inverse of a.
   $$7 \cdot 7^{-1} x = 6 \cdot 7^{-1} \pmod{9}$$
   $$x = 6 \cdot 7^{-1} \pmod{9}$$

$(7 \times c) \bmod n = 1$

$(7 \times c) \bmod 9 = 1$

$c=1)\ 7 \bmod 9 \neq 1$

$c=2)\ 14 \bmod 9 \neq 1$

$c=3)\ 21 \bmod 9 \neq 1$

$\boxed{c=4)}\ 28 \bmod 9 = 1$ ✓

$x \equiv 6.4 \bmod 9$

$x = 24 \bmod 9$

$\boxed{x_0 = 6}$

6) General solⁿ eqⁿ is

$x_K = x_0 + K\left(\frac{n}{d}\right)$

$x_1 = 6 + 1\left(\frac{18}{2}\right) = 6 + 9 = \underline{15}$.

---

2) Solve $9x \equiv 12 \pmod{15}$

Solⁿ $\gcd(9, 15) = 3$.

$\therefore$ The no of possible solⁿ are 3.

The given congruence is equivalent to

$3x \equiv 4 \pmod 5$

$5 / 3x - 4$

$\Rightarrow 3x - 4 = 5k$

$\Rightarrow x = \frac{5k+4}{3}$

If $k = 1$; $x = 3$

$x \equiv 3 \pmod 5$

The G.S is

$x_K = x_0 + k\left(\frac{m}{d}\right)$

$x_K = 3 + k\left(\frac{15}{3}\right)$

$x_K = 3 + 5k$

$\therefore x = \underline{\underline{3, 8, 13}}$.

* The chinese Remainder Theorem :-

The chinese Remainder Theorem (CRT) is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below:

$X \equiv a_1 (\mod m_1)$; $X \equiv a_2 (\mod m_2)$; $X \equiv a_3 (\mod m_3)$ - - - - $X \equiv a_n (\mod m_n)$.

CRT states that the above equations have a unique solution of the moduli are relatively prime.

$$\boxed{X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \dots + a_n M_n M_n^{-1}) \mod M}$$

1) Solve the following equations using CRT

$X \equiv 2 (\mod 3)$

$X \equiv 3 (\mod 5)$

$X \equiv 2 (\mod 7)$

Soln: $X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \mod M$

Given		To find		
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	$M = 105$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$; $M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$; $M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$M_1 \times M_1^{-1} = 1 \mod m_1$

Multiplicative inverse

$35 \times M_1^{-1} = 1 \bmod 3$; $M_2 \times M_2^{-1} = 1 \bmod m_2$; $M_3 \times M_3^{-1} = 1 \bmod m_3$

By inspection, $M_1^{-1} = 1$ ✗ Re-(1)

$21 \times M_2^{-1} = 1 \bmod 5$; $15 \times M_3^{-1} = 1 \bmod 7$

$35 \times 2 = 1 \bmod 3$; $21 \times 1 = 1 \bmod 5$; $15 \times 1 = 1 \bmod 7$

$M_1^{-1} = 2$; $M_2^{-1} = 1$; $M_3^{-1} = 1$.

$\therefore X = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$X = 233 \bmod 105$

$X = 23$.

$$105 \overline{)233} (2$$
$$\frac{210}{23}$$

---

2) Solve the following equations using CRT:

$4x \equiv 5 (\bmod 9)$

$2x \equiv 6 (\bmod 20)$.

Soln: $4x \equiv 5 (\bmod 9)$; $2x \equiv 6 (\bmod 20)$

x^{ly} by 4^{-1} on both sides. ; $\div$ by $\overset{2\times3}{2}$

$4^{-1} \times 4x \equiv 4^{-1} \times 5 (\bmod 9)$; $x \equiv 3 (\bmod 10)$

$x \equiv 4^{-1} (\bmod 9) \times 5 (\bmod 9)$

↑ x'liplicative inverse
1 as the remainder

$x = 7 \times 5 (\bmod 9)$

$x \equiv 35 (\bmod 9)$

$x \equiv 8 (\bmod 9)$

$\therefore$ $x \equiv 8 (\bmod 9)$

$x \equiv 3 (\bmod 10)$

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_1^{-1})$

Given		To Find		
$a_1 = 8$	$m_1 = 9$	$M_1 = 10$	$M_1^{-1} = 1$	$M = 90$
$a_2 = 3$	$m_2 = 10$	$M_2 = 9$	$M_2^{-1} = 9$	

$M = m_1 \times m_2 = 9 \times 10 = 90$

$M_1 = \frac{M}{m_1} = \frac{90}{9} = 10$; $M_2 = \frac{M}{m_2} = \frac{90}{10} = 9$

$M_1 \times M_1^{-1} = 1 \bmod m_1$; $M_2 \times M_2^{-1} \equiv 1 \bmod m_2$

$10 \times M_1^{-1} \equiv 1 \bmod 9$; $9 \times M_2^{-1} \equiv 1 \bmod 10$

$10 \times 1 \equiv 1 \bmod 9$; $9 \times 9 \equiv 1 \bmod 10$

$\underline{\underline{M_1^{-1} = 1}}$; $\underline{\underline{M_2^{-1} = 9}}$

$\therefore X = (8 \times 20 \times 1 + 3 \times 9 \times 9) \bmod 180$

$X \equiv 403 \bmod 180.$

$\underline{\underline{X \equiv 43}}$

---

3) Solve the following equations using CRT:

$X \equiv 5 \pmod 3$

$X \equiv 2 \pmod 5$

$X \equiv 1 \pmod{11}.$

Solⁿ : $X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$.

Given		To find		
$a_1 = 5$	$m_1 = 3$	$M_1 = 55$	$M_1^{-1} = 1$	
$a_2 = 2$	$m_2 = 5$	$M_2 = 33$	$M_2^{-1} = 2$	$M = 165$
$a_3 = 1$	$m_3 = 11$	$M_3 = 15$	$M_3^{-1} = 3$	

$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 11 = 165$

$M_1 = \frac{M}{m_1} = \frac{165}{3} = 55$; $M_2 = \frac{M}{m_2} = \frac{165}{5} = 33$; $M_3 = \frac{M}{m_3} = \frac{165}{11} = 15$

$M_1 \times M_1^{-1} \equiv 1 \bmod m_1$; $M_2 \times M_2^{-1} \equiv 1 \bmod m_2$; $M_3 \times M_3^{-1} \equiv 1 \bmod m_3$

$55 \times M_1^{-1} \equiv 1 \bmod 3$; $33 \times M_2^{-1} \equiv 1 \bmod 5$; $15 \times M_3^{-1} \equiv 1 \bmod m_3$

$55 \times 1 \equiv 1 \bmod 3$; $33 \times 2 \equiv 1 \bmod 5$; $15 \times 3 \equiv 1 \bmod 11$

$\underline{\underline{M_1^{-1} = 1}}$; $\underline{\underline{M_2^{-1} = 2}}$; $\underline{\underline{M_3^{-1} = 3}}$

$\therefore x = (5\times 55\times 1 + 2\times 33\times 2 + 1\times 15\times 3) \bmod 165$

$x = 452 \bmod 165$

$x = 122$

---

4) Solve $3^{302} \bmod 5005$ using CRT.

$M = 5005$

$M = 5\times 7\times 11\times 13$.

$m_1 = 5,\ m_2 = 7,\ m_3 = 11,\ m_4 = 13$.

$M_1 = \frac{M}{m_1} = \frac{5005}{5} = 1001$; $M_2 = \frac{M}{m_2} = \frac{5005}{7} = 715$

$M_3 = \frac{M}{m_3} = \frac{5005}{11} = 455$; $M_4 = \frac{M}{m_4} = \frac{5005}{13} = 385$.

To find a_i values:

$a_i = 3^{302} \bmod m_i$.

$a_1 = 3^{302} \bmod m_1(5) = 4$.

$a_2 = 3^{302} \bmod 7 = 2$

$a_3 = 3^{302} \bmod 11 = 9$

$a_4 = 3^{302} \bmod 13 = 9$

$3^{302} \bmod 5 = 3^{60\times 5+2} \bmod 5$

$= (3^5)^{60} . 3^2 \bmod 5$

$5) \, 302 \, (60$
$\underline{300}$
2

$= (3)^{60} . 3^2 \bmod 5 \quad (a^p \bmod p = a)$.

$= 3^{62} \bmod 5$

$= 3^{12\times 5+2} \bmod 5 = (3^5)^{12} . 3^2 \bmod 5$

$= (3)^{12} . 3^2 \bmod 5$

$= 3^{14} \bmod 5$

(OR)

302 as multiple of 4

$= 3^{5\times 2+4} \bmod 5$

$= (3^5)^2 . 3^4 \bmod 5$

$= 3^6 \bmod 5$

$= 3^{5\times 1+1} \bmod 5$

$= (3^5) 3 \bmod 5$

$= 3.3 \bmod 5 = 4$

$M_1 \times M_1^{-1} = 1 \bmod m_1$; $M_2 \times M_2^{-1} = 1 \bmod 7$; $M_3 \times M_3^{-1} = 1 \bmod 11$

$1001 \times M_1^{-1} \equiv 1 \bmod 5$; $715 \times M_2^{-1} \equiv 1 \bmod 7$; $455 \times M_3^{-1} = 1 \bmod 11$

$1001 \times 1 \equiv 1 \bmod 5$; $715 \times 1 = 1 \bmod 7$; $455 \times 3 = 1 \bmod 11$

$\underline{M_1^{-1} = 1}$; $\underline{M_2^{-1} = 1}$; $\underline{M_3^{-1} = 3}$

$M_4 \times M_4^{-1} = 1 \bmod 13$

$385 \times M_4^{-1} \equiv 1 \bmod 13$

$385 \times 5 \equiv 1 \bmod 13$

$\underline{M_4^{-1} = 5}$.

$\therefore\ x = (4 \times 1 \times 1001 + 2 \times 1 \times 715 + 9 \times 3 \times 455 + 5 \times 9 \times 385) \bmod 5005$

$x = 35044 \bmod 5005$

$\underline{x = 9}$.

---

5) Solve the following equations using CRT

a) $x \equiv 3 \bmod 4$
$x \equiv 2 \bmod 3$
$x \equiv 4 \bmod 5$

b) $2x \equiv 6 \pmod{14} \div 2$.
$3x \equiv 9 \pmod{15} \div 3$
$5x \equiv 20 \pmod{60} \div 5$
$\gcd(2,14) = 2$.

---

6) Find a number having remainder 2, 3, 4, 5 when divided by 3, 4, 5, 6 respectively.

Sol^n:
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 4$
$x \equiv 4 \pmod 5$
$x \equiv 5 \pmod 6$

Linear Diophantine Equation :-

An equation of the form $ax+by+c=0$ where $a\neq 0, b\neq 0$ and c is an integers is called a linear diophantine eq^n in two variables x & y.

Eg:- i) $8x+17y=7$ ii) $2x+3y=12$.

Solution of Linear Diophantine Equation :-

A pair (x_0, y_0) of integers is called a sol^n of linear Diophantine equation $ax+by=c$ if $ax_0+by_0=c$ and $(a,b)=d$.

then the general solution is given by

$$\boxed{x_1 = x_0 - \frac{b}{d}t \;;\; y_1 = y_0 + \frac{a}{d}t}$$

---

1. Which of the following Diophantine equation cannot be solved.

i) $6x+51y=22 \rightarrow (1)$

By Euclidean Algorithm.

$51 = 3 + 6\times 8$.

$6 = 0 + 3\times 2$.

$$\begin{array}{r} 6\overline{)51}(8 \\ \underline{48} \\ 3\overline{)6}(2 \\ \underline{6} \\ 0 \end{array}$$

gcd of $(6,51) = 3$.

$3 \nmid 22$.

$\therefore$ eq^n (1) is not solvable.

---

ii) $33x+14y=115 \rightarrow (1)$

$33 = 5 + 14\times 2$

$14 = 4 + 5\times 2$

$5 = 1 + 4\times 1$

$4 = 0 + 1\times 4$

$\gcd(14,33) = 1$ &

$1 / 115$

So, eqⁿ (1) is solvable.

$$
\begin{array}{l}
14)\,33\,(2 \\
\quad 28 \\
\hline
\quad 5)\,14\,(2 \\
\qquad 10 \\
\hline
\qquad 4)\,5\,(1 \\
\qquad\quad 4 \\
\hline
\qquad\quad 1)\,4\,(4 \\
\qquad\qquad 4 \\
\hline
\qquad\qquad 0
\end{array}
$$

---

2. Determine all the solution in +ve integers of the linear Diophantine equation, $54x+21y=906$.

Solⁿ:- Given L.D. eqⁿ

$$54x + 21y = 906.$$

By Euclidean Algorithm

$54 = 12 + 21\times 2$

$21 = 9 + 12\times 1$

$12 = 3 + 9\times 1$

$9 = 0 + 3\times 3$

$\gcd(21, 54) = 3$ &

$3/906.$

So, eqⁿ(1) is solvable.

$$
\begin{array}{l}
21)\,54\,(2 \\
\quad 42 \\
\hline
\quad 12)\,21\,(1 \\
\qquad 12 \\
\hline
\qquad 9)\,12\,(1 \\
\qquad\quad 9 \\
\hline
\qquad\quad 3)\,9\,(3 \\
\qquad\qquad 9 \\
\hline
\qquad\qquad 0
\end{array}
$$

---

3) Find the general solⁿ of the eqⁿ

$70x + 112y = 168$.

Solⁿ :- $\gcd(70, 112) =$

$112 = 70 \times 1 + 42$

$70 = 42 \times 1 + 28$

$42 = 28 \times 1 + 14$

$28 = 14 \times 2 + 0$.

$$\begin{array}{l} 70)\,112\,(1 \\ \underline{70} \\ 42)\,70\,(1 \\ \underline{42} \\ 28)\,42\,(1 \\ \underline{28} \\ 14)\,28\,(2 \\ \underline{28} \\ 0 \end{array}$$

$\therefore \gcd(70, 112) = 14$.

Now $14 / 168 = \underline{12}$.

$\therefore$ Linear Diophantine eqⁿ $70x + 112y = 168$ has a solution.

By reverse.

$14 = 42 - 28$

$= 42 - (70 - 42)$

$= 42 - 70 + 42$

$= 2(42) - 70$

$= 2(112 - 70) - 70$

$= 2(112) - 2(70) - 70$

$14 = 2(112) - 3(70)$

Multiply by 12.

$14(12) = (2(12)112 - 3(12)70$.

$168 = \underline{24} \cdot 112 - \underline{36} \cdot 70 \Rightarrow 168 = -\underline{36} \cdot 70 + \underline{24} \cdot 112$

Thus $y_0 = 24$ & $x_0 = -36$ is a particular solⁿ of the given eqⁿ.

The General solⁿ is given by

$x_1 = x_0 + \frac{b}{d} t$ $\qquad y_1 = y_0 - \frac{a}{d} t$

(put both +)

$x_1 = -36 + \left(\frac{112}{14}\right)t$; $y_1 = 24 - \left(\frac{70}{14}\right)t$

$x_1 = -36 + 8t$; $y_1 = 24 - 5t$.

Hence, $x_1 = -36 + 8t$ & $y_1 = 24 - 5t$, t is an integer.

---

4) $39x - 56y = 11$.

$56 = 39 \times 1 + 17$

$39 = 17 \times 2 + 5$

$17 = 5 \times 3 + 2$

$5 = 2 \times 2 + 1$

$2 = 1 \times 2 + 0$

$$
\begin{array}{l}
39)\,56\,(1 \\
\quad 39 \\
\quad 17)\,39\,(2 \\
\qquad 34 \\
\qquad 5)\,17\,(3 \\
\qquad\quad 15 \\
\qquad\quad 2)\,5\,(2 \\
\qquad\qquad 4 \\
\qquad\qquad 1)\,2\,(2 \\
\qquad\qquad\quad 2 \\
\qquad\qquad\quad 0
\end{array}
$$

Hence $\gcd(39, 56) = 1$

Now $1 / 11 = \underline{11}$.

$\therefore$ Linear Diophantine eqn $39x - 56y = 11$ has a solution.

By reverse,

$1 = 5 - 2(2)$.

$1 = 5 - 2(17 - 3(5))$

$1 = 5 - 2(17) + 6(5)$

$1 = 7(5) - 2(17)$

$1 = 7(39 - 2(17)) - 2(17)$

$1 = 7(39) - 14(17) - 2(17)$

$1 = 7(39) - 16(17)$

$1 = 7(39) - 16(56 - 1(39))$

$1 = 7(39) - 16(56) + 16(39)$

$1 = 23(39) - 16(56)$

Multiply by 11

$$1(11) = 23(11)(39) - 16(11)(56)$$
$$11 = \underbrace{253}_{x_0}(39) - \underbrace{176}_{y_0}(56).$$

thus $x_0 = 253$, $y_0 = 176$. is a particular solⁿ of the given eqⁿ.

Its general solⁿ is

$x_1 = x_0 + \frac{b}{d}t$; $y_1 = y_0 - \frac{a}{d}t$ (put both +)

$x_1 = 253 + \left(-\frac{56}{1}\right)t$; $y_1 = 176 - \left(\frac{39}{1}\right)t$.

$x_1 = 253 - 56t$; $y_1 = 176 - 39t$

Hence $x_1 = 253 - 56t$ & $y_1 = 176 - 39t$; t is an integer.

---

5) Solve : $7x + 18y = 208$. $x_0 = -1040$; $y_0 = 416$

6) Solve : $56x + 72y = 40$. $x_0 = 20$; $y_0 = -15$.

7) Solve : $172x + 20y = 1000$.

---

8) A Certain number of Sixes and nines is added a sum of 126. if the number of sixes and is interchanged, the new sum is 114. How many each were there Originally?

Solⁿ :- Let x be no of sixes.

y be no of nines.

$$6x + 9y = 126.$$
$$9x + 6y = 114.$$

$9 = 3 + 6 \times 1$

$6 = 0 + 3 \times 2$

$\gcd(6, 9) = 3$.

$3 / 126 = \underline{\underline{42}}$.

$$\begin{array}{r|l} 6) & 9(1 \\ & \underline{6} \\ 3) & 6(2 \\ & \underline{6} \\ & 0 \end{array}$$

Reverse.

$3 = 9 - 6 \times 1$

$3 = 6(-1) + 9(1)$

$3.42 = 6((-1)(42)) + 9((1)(42))$

$126 = 6(-42) + 9(42)$

$x = -42 + 3t \geq 0 \qquad y = 42 - 2t \geq 0$.

$3t \geq 42 \qquad -2t > -42$

$t \geq 14 \qquad 2t \geq 42$

$t < 21$.

$14 < t < 21$.

$x = x_0 + \frac{q}{d} t \qquad y = y_0 - \frac{p}{d} t$

$x = 3t \qquad y = 14 - 2t$.

t	x	y
14	0	14

Initial value

To Find the value of t S.T

$6y + 9x = 114$.

$6(14 - 2t) + 9(3t) = 114$.

$15t - 30 = 0$

$15t = 30$

$\underline{\underline{t = 2}}$.

$x_0 = 3t \qquad y_0 = 14 - 2t$

$\underline{\underline{x_0 = 6}} \qquad \underline{\underline{y_0 = 10}}$.